1nQ Cookie Policy

Last updated October 8, 2026

This Cookie Policy explains how 1nQ Inc. ("Company," "we," "us," or "our") uses cookies and similar technologies to recognize you when you visit our website at https://1nq.ai, use the 1nQ Platform, or interact with conversational AI Agents hosted on our platform (collectively, the "Services").

This policy explains what these technologies are, why we use them, and your rights to control our use of them. This Cookie Policy forms part of our broader [Privacy Policy], which explains how we protect your personal data more generally.

---

1. What are cookies?

Cookies are small data files that are placed on your computer or mobile device when you visit a website or use an online platform. Cookies are widely used by online service providers in order to make their websites or services work, or to work more efficiently, as well as to provide reporting information.

- **First-party cookies:** Cookies set by the website or platform owner (in this case, 1nQ Inc.).
- **Third-party cookies:** Cookies set by parties other than the website owner. These enable third-party features or functionality to be provided on or through the website (e.g., interactive content, analytics, and advertising).
- **Session cookies:** Temporary cookies that expire and are deleted when you close your browser.
- **Persistent cookies:** Cookies that remain on your device for a set period of time or until you manually delete them.

---

2. Why do we use cookies?

We use first-party and third-party cookies for several reasons. Some cookies are required for technical reasons in order for our Services to operate, and we refer to these as "essential" or "strictly necessary" cookies. Other cookies enable us to track and target the interests of our users to enhance the experience on our Services. Third parties serve cookies through our Services for analytics, advertising, and other purposes.

The specific types of first-party and third-party cookies served through our Services and the purposes they perform are described below.

---

3. Types of Cookies We Use

A. Essential (Strictly Necessary) Technologies

These technologies are strictly necessary to provide you with services available through our Platform and to use some of its features. Because they are strictly necessary to deliver the Services, you cannot refuse them without impacting how our Services function.

Name	Type	Purpose	Duration	Can you refuse?
`theme`	localStorage (first-party)	Stores your chosen platform theme (dark/light/high-contrast)	Persistent	No (strictly necessary)
`preferredLanguage`	localStorage (first-party)	Stores your chosen platform language locale	Persistent	No (strictly necessary)
`user`	localStorage (first-party)	Stores your authenticated session profile (name, email, preferences) so the platform can restore your session	Persistent (cleared on logout)	No (strictly necessary)
`chatTTSEnabled`	localStorage (first-party)	Remembers your text-to-speech preference for Agent conversations	Persistent	No (functional preference)
`authContextInitialized`	sessionStorage (first-party)	Prevents duplicate authentication initialisation within a browser tab	Session	No (strictly necessary)
`jwt`	Cookie (first-party, HttpOnly, Secure)	Short-lived access token for authenticating API requests. Set by the server; not accessible to JavaScript.	Short-lived (minutes)	No (strictly necessary)
`refreshToken`	Cookie (first-party, HttpOnly, Secure, path-restricted to /api/auth/refresh)	Short-lived access token for authenticating API requests. Set by the server; not accessible to JavaScript.	Days (configurable)	No (strictly necessary)

`Stripe cookies`	Cookie (third-party, set by Stripe.js)	Long-lived refresh token for maintaining your session across browser tabs and page reloads. Set by the server; not accessible to JavaScript.	Days (configurable)	No (strictly necessary)
`CSRF token`	Custom HTTP header (first-party)	A short-lived signed token sent in request headers to protect against cross-site request forgery attacks. Not stored as a cookie — held in application memory only.	1 hour	No (strictly necessary)
`Cloudflare Turnstile`	Cookie + localStorage (third-party, Cloudflare)	Bot detection and CAPTCHA verification during account registration and form submissions. Cloudflare may set cookies such as cf_clearance and use localStorage for challenge state.	Varies (session to 30 minutes)	No (strictly necessary)

B. Analytics and Marketing Technologies

These technologies collect information that is used to help us understand how our Services are being used, to measure site usage, and to attribute and track advertising campaigns.

Name	**Type**	**Purpose**	**Duration**	**Can you refuse?**
_ga, _ga_*	Cookie (third-party, Google)	Google Analytics 4 — site usage measurement	Up to 2 years	Yes
li_fat_id	Cookie + localStorage (first-party, LinkedIn)	LinkedIn ad attribution identifier	2 years	Yes

4. What about other tracking technologies, like localStorage and web beacons?

Cookies are not the only way to recognise or track visitors to a website. As noted in the tables above, we also use **localStorage**, which is a web storage technology that allows a website or application to store data locally within your web browser. Unlike cookies, localStorage data is not automatically sent to the server with every HTTP request, and it does not have an automatic expiration date (it persists until manually cleared). We use localStorage primarily for essential preferences, such as remembering your chosen theme (theme) and language (preferredLanguage), as well as for certain marketing attributions (li_fat_id).

We may also use **web beacons** (sometimes called "tracking pixels" or "clear gifs"). These are tiny graphics files that contain a unique identifier that enable us to recognise when someone has visited our Services or opened an email that we have sent them. This allows us to monitor traffic patterns, understand whether you have come to our Services from an online advertisement, and measure the success of email marketing campaigns. In many instances, these technologies are reliant on cookies to function properly, and so declining cookies will impair their functioning.

We also use a CSRF (Cross-Site Request Forgery) protection token, which is a short-lived cryptographic token sent in custom HTTP request headers. This token is held in application memory only (not as a cookie or in browser storage) and is used solely to verify that requests to our servers originate from our own platform. It contains no personal data and expires after one hour.

---

5. How can you control cookies?

You have the right to decide whether to accept or reject cookies. You can exercise your cookie rights by setting your preferences in the Cookie Consent Manager that appears when you first visit our website. The Cookie Consent Manager allows you to select which categories of cookies you accept or reject. Essential cookies cannot be rejected as they are strictly necessary to provide you with services.

You can also change your cookie preferences at any time using the "Cookie Settings" link at the bottom of the page.

Browser Controls: You can set or amend your web browser controls to accept or refuse cookies. If you choose to reject cookies, you may still use our website, though your access to some functionality and areas of our website (such as maintaining a continuous Agent conversation session) may be restricted. As the means by which you can refuse cookies through your web browser controls vary from browser-to-browser, you should visit your browser's help menu for more information.

Global Privacy Control (GPC): We recognise and honour Global Privacy Control (GPC) signals. If you use a browser or extension that supports GPC, we will treat this as a valid request to opt out of the sale or sharing of your personal information for targeted advertising purposes via cookies under applicable state privacy laws, including the California Consumer Privacy Act (CCPA).

Google Analytics Opt-Out: To opt out of being tracked by Google Analytics across all websites, visit http://tools.google.com/dlpage/gaoptout.

---

6. How often will we update this Cookie Policy?

We may update this Cookie Policy from time to time in order to reflect, for example, changes to the cookies we use or for other operational, legal, or regulatory reasons. Please therefore revisit this Cookie Policy regularly to stay informed about our use of cookies and related technologies.

The date at the top of this Cookie Policy indicates when it was last updated.

---

7. Where can you get further information?

If you have any questions about our use of cookies or other technologies, please email us at foi@1nq.ai or contact us by post at:

1nQ Inc.

1111b South Governors Avenue

Dover

Delaware

19904

United States